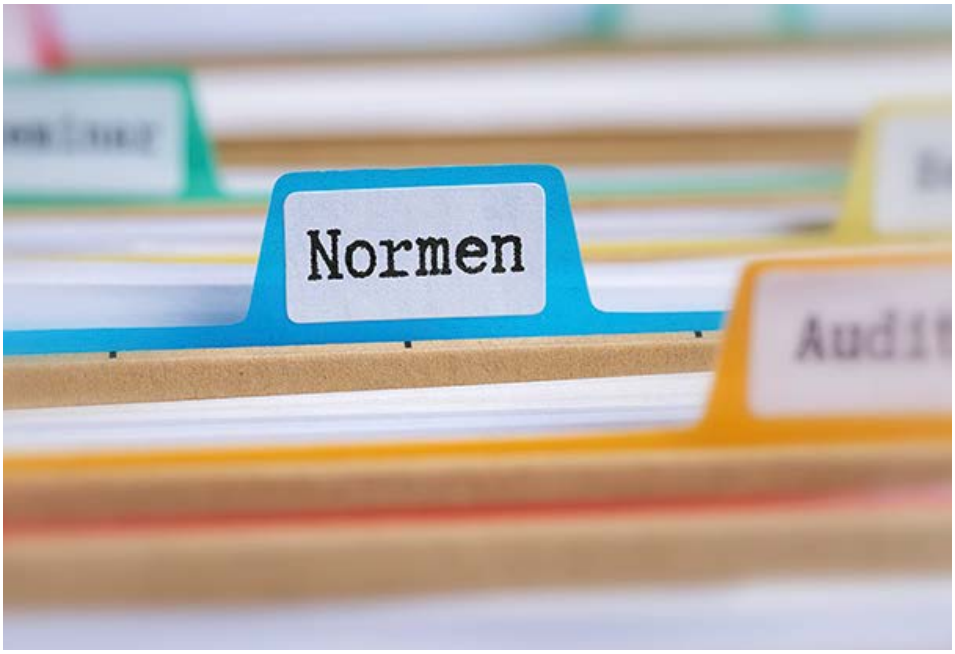
Normung im Compliance-Bereich

In seinem Gastbeitrag gibt Prof. Dr. Bartosz Makowicz einen Überblick über die Normungsvorhaben im Bereich „Governance und Compliance". Es entsteht derzeit für den Bereich eine systematisch geordnete Reihe von Managementsystem-Normen.

privat

Prof. Dr. Bartosz Makowicz ist Universitätsprofessor und Direktor des Viadrina Compliance Center (VCC), einer interdisziplinären Forschungseinrichtung an der Europa-Universität Viadrina Frankfurt(O).



© IMAGO / Shotshop

Das Register an Normungen im Bereich Compliance wächst.

Der Gesetzgeber scheint seine Chance, endlich fundierte Gesetzesgrundlagen für Compliance zu setzen, wieder einmal verpasst zu haben. Zwar ist es ihm immerhin mit dem GWB-Digitalisierungsgesetz gelungen, die vom Bundeskartelamt vehement abgelehnte Compliance-Defense zu kodifizieren, aus den zwei Hauptvorhaben wird aber wohl in der Legislaturperiode nichts mehr: Während das Verfahren zum VerSanG-E endgültig ins Stocken geraten ist, wird vor der Sommerpause kaum noch ein konsensfähiger Entwurf des Umsetzungsgesetzes zur Hinweisgeberschutz-Richtlinie vorgelegt.

Ganz anders sieht die Lage dagegen bei der International Organization for Standardization (ISO) aus, die sich seit 2012 intensiver mit Normung auch im Compliance-Bereich beschäftigt. Dies nicht zu Unrecht, beachte man die diversen Vorteile der Standardisierung. Sie sorgen für Vereinheitlichung der Prozesse und Strukturen, Beschleunigung des Wirtschaftsverkehrs, schaffen Vertrauen und Sicherheit und generieren so einen Wettbewerbsvorteil. Nicht zuletzt können sie auch in einem Haftungsprozess als sog. antizipierte Sachverständigengutachten (im Sinne von „Stand der Technik") herangezogen werden.

Den Katalog eröffnet der Leitfaden ISO 37000 Governance of Organizations, in dem die Grundsätze für Governance von Organisationen festgelegt werden. Für das systematische Verständnis ist es wichtig zu betonen, dass es sich bei Governance („doing the *right* things") um eine den Managementsystemen („*doing* the things right") übergeordnete Ebene handelt. Die Norm befindet sich derzeit in der finalen Abstimmungsrunde und soll im Herbst 2021 veröffentlicht werden. Parallel sind weitere Initiativen mit dem Ziel gestartet, ISO 37000 um Normen zur Messung der Effektivität der umgesetzten Governance-Lösungen zu ergänzen.

Die im April dieses Jahres veröffentlichte ISO 37301 könnte systematisch darunter eingestuft werden. In ihr wurden Anforderungen an Compliance-Management-Systeme (CMS) festgelegt. Es handelt sich bei ISO 37301 um die Nachfolgerin der ISO 19600, die im Zuge der Aktualisierung nicht nur eine neue Hausnummer erhalten hat. Geändert wurde auch der Typ der Norm von B in A, was bedeutet, dass CMS künftig nach ISO 37301 zertifiziert werden können. Derzeit werden noch besondere Anforderungen erarbeitet, die Zertifizierungsstellen erfüllen müssen. Ferner wurde die Norm an mehreren Stellen angepasst und optimiert. Besondere Compliance-Themenfelder werden dagegen in anderen Standards behandelt. Dies gilt etwa für die Korruptionsprävention, die in der 2016 erschienenen ISO 37001 Anti-Bribery Management Systems festgelegt sind und zu der in diesem Jahr ein Handbuch veröffentlicht wurde.

Im letzten Stadium befindet sich ebenfalls die Normung des Leitfadens ISO 37002 Whistleblowing Management Systems (WMS). Das Timing könnte nicht besser sein, denn mit der Ausgabe der Norm ist bereits im Herbst, also noch vor Umsetzung der eingangs erwähnten Hinweisgeberschutz-Richtlinie, zu rechnen. Die geplante Norm könnte in dem Zusammenhang deutlich an Bedeutung gewinnen, da weder die Richtlinie selbst, noch (jedenfalls voraussichtlich) das deutsche Umsetzungsgesetz konkrete Implementierungshinweise enthalten werden. Inhaltlich abgerundet wird die ISO 37002 durch eine technische Spezifizierung zu internen Untersuchungen. Das Verfahren ist im Juni auf den Weg gebracht worden. Dies schließt auch zunächst den Katalog an ISO-Normen im Bereich Governance und Compliance. Vor dem Hintergrund bleiben aber zwei wesentliche Punkte erwähnenswert.

Zum einen die Frage nach der Zertifizierung von CMS. Die Anwendung eines Standards, dies vorab, muss nicht automatisch mit einer Zertifizierung einhergehen. Vielmehr können Organisationen diese als einen Leitfaden oder Checkliste nutzen, um die implementierten Lösungen zu evaluieren oder um sich bei Erstimplementierung den Überblick zu verschaffen. Hinsichtlich einer Zertifizierung sollen dagegen Vor- und Nachteile abgewogen werden. Vorteilhaft ist sicherlich die objektive Sicht (des Prüfers), die zur Systemoptimierung führen kann. Ein Zertifikat kann ebenfalls einen Wettbewerbsvorteil bescheren. Anderseits sind aber Zertifizierungsverfahren formalistisch geprägt, kostspielig, haben kaum eine rechtliche Bedeutung und führen sicherlich per se nicht zur Enthaftung (eine Indizwirkung kann womöglich angenommen werden).

Zum anderen kann wegen der neuen Zertifizierungsmöglichkeit der ISO 37301 das bisher komplementäre Verhältnis zu PS 980 ins Schwanken geraten. Ein Prüfungsstandard wird dann nämlich nicht mehr benötigt, was für eine rege Konkurrenz zwischen Wirtschaftsprüfern und Zertifizierungsstellen sorgen kann. Produktiver dagegen könnte das Verhältnis zu den in den letzten beiden Jahren erschienenen DICO-Standards sein, die – anders als ISO-Normen – die nationale Rechtslage und die hierzulande vorherrschende Praxis berücksichtigen, zugleich aber auch gegenüber den ISO-Normen anschlussfähig bleiben.

Es bleibt zu hoffen, dass in der neuen Legislaturperiode in puncto Compliance entschlossener und konsequenter vorgegangen wird. Standards werden Gesetze nie ersetzen, sie können aber als anerkannter Stand der Technik bestens die Lücken füllen und eine verlässliche Orientierung für Organisationen bieten. *Prof. Dr. Bartosz Makowicz*